# Security Awareness Training

## Source

This training material is taken from Iowa's *Securing the Human* online material unless otherwise cite. This information has been adapted to fit the training requirements of Iowa Child Advocacy Board volunteers.

## Purpose

The Iowa Child Advocacy Board's CASA and FCRB programs handle a great deal of confidential information and its volunteers are given access to that information, electronically or in hard copy. It is critical that all volunteers understand the responsibility that comes with having access to confidential information and the significance of protecting that information at all times. Your understanding and following of our data security policies are key to securing our sensitive information and our organization.

## Key Elements to understand


- Data protection
- Email and Texting use
- Internet use
- Social Engineering
- Data retention
- Data disposal
- Incident reporting
- Wi-Fi
- Working remotely
- Mobile device and removable media security
- Encryption
- Passwords
- Physical security
- Social networks
- Protecting your personal computer
- Personally identifiable information (PII)
- Cloud computing

## Data Protection

A great deal of our security focuses on keeping your devices secure. While this is important, understand that most attackers are not after your devices but the sensitive information that resides on them. Examples of sensitive information as it pertains to ICAB volunteers can include case file documents, notes and personally identifiable information. As such, you should take the following steps when handling sensitive information:

- Always understand the sensitivity of the information you are working with. If you are uncertain about the sensitivity of any information or the steps you should take to secure it, ask your local coordinator.

- Only use systems authorized by ICAB to store, process or transmit sensitive information. Do not copy or store sensitive information to any unauthorized systems or accounts, such as personal laptops or personal email accounts.

- Only log into ICAB's online data system with your unique user ID.

- If you believe any sensitive data has been lost, stolen or compromised be sure to contact your local coordinator immediately. The sooner our organization is notified, the quicker we can respond to minimize damage.

Additional steps are addressed throughout this handout.

## Email and Texting use

Email is one of the most powerful weapons in the cyber attacker's arsenal, simply because so many people depend on it in their daily lives. With email, an attacker can easily pretend to be someone or something you trust, such as your friend or a credible organization. Terms to understand:

- Phishing: Attacks that work by tricking you into doing something seemingly harmless, like clicking on a link or opening an attachment.

- Spear phishing: This is a highly targeted attack where only a few emails are sent to specific individuals within an organization that appears realistic,

often with a subject that is relevant to the victim's job or appear to come from individuals that the victim highly trusts.

- Messaging: Just like email, almost any type of messaging can be used for phishing attacks, such as those on Facebook, Skype, Twitter or your smartphone. Always be careful of messages, regardless of what technology you use.

Safely using email and messaging is ultimately about common sense. Assume every email or text you send can become public. Confidential case information needs to be protected when using email and messaging. Do not use names or other identifying information in an email, texts or other messaging programs. Those records can be accessed and made public.

## Internet Use

Browsers are one of the primary ways we interact with the Internet. They also provide a window into our computers and are one of the most dangerous applications we use.

If your browser or any of your plugins are outdated or vulnerable, your computer will most likely become infected. Unfortunately, there is no simple way to tell if a website is safe or not, so it is important to take some simple precautions.

- First, most browsers maintain a list of known malicious websites that intend to cause you harm. If you accidently visit one of these known websites, your browser will post a warning like you see here. If your browser warns you against visiting a website like this, do not connect to it.
- Always use the most current version of your browser and ensure it is up-to-date. This prevents attackers from exploiting known weaknesses and is one of the most effective ways to protect yourself.
- Be sure your connection is encrypted whenever you connect to sensitive websites, such as online banking. Look for signs of encryption like the website address starting with HTTPS and a padlock icon in the status bar.
- Finally, always be sure to scan any files you download with anti-virus.

## Social Engineering

Social engineering is nothing more than an attacker building trust with you, then abusing that trust to get what they want.

- If you get an email, message or phone call that seems odd, suspicious or too good to be true, it may be an attack.
- Common indicators of a social engineering attack include people asking for information they should not have access to, using a lot of confusing or technical terms or creating a sense of urgency.
- If you believe someone is attempting to trick or fool you, simply hang up the phone or ignore the email.

## Data Retention

Good management of records is critical for our organization to fulfill its mission. Our records are an asset. They help us run our operations and satisfy our legal responsibilities. Records can be paper or electronic. Paper records include case file documents and reports while electronic records include case records in a database, email, or voicemail.

Email is often considered just as legally binding as a paper letter. Many of our emails are considered significant, official records of the organization. As such, the following are generally applicable advice and guidelines:

- Be mindful that any record you make could be discovered through litigation or leaked to the public. So before you send an email or a text message, pause and ask yourself how it would appear if it were produced in court or printed in the newspaper. Assume every email or text you send can become public.
- Don’t assume that the deletion of an unfavorable electronic record will be the end of it. Deletion of an electronic record does not always mean it is unrecoverable.
- We destroy records when they are no longer needed or required. However, we do not condone the destruction, falsification or concealment of records for the purpose of covering up illegal or embarrassing conduct.

## Data Disposal

The goal of disposing data is to ensure that it cannot be recovered. Unfortunately, it's not that simple with digital data. When you dispose of a device, such as donating your old smartphone or selling a computer on eBay, there is most likely sensitive information still on those devices. Any device that has sensitive information must have that data wiped before it is disposed of.

Many people mistakenly believe they can simply delete data and that the data is gone. Unfortunately, this is not true. When you delete a file it is actually still on your device and can be easily recovered. Depending on the options used, even formatting a drive is not sufficient to securely delete all data.

One of the few ways you can securely destroy digital data is to use special programs that overwrite or wipe every bit on the storage device. Be sure to always securely dispose of any confidential information.

## Incident Reporting

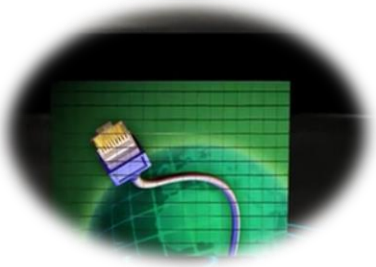
If you believe your computer, mobile device or email account has been compromised, do not attempt to fix the problem yourself. Instead, stop using it and seek tech assistance immediately. Play it safe. It is far better to report a system that is not compromised than it is to fail to report a system that is compromised.

Unfortunately, there is no simple way to determine if you are hacked. However, here are some things you can look for as indicators you have been hacked.

- First, your anti-virus generates an alert. If it finds a virus on your system, your computer may have been hacked.
- Second, your browser is taking you to unwanted websites or random websites open on your screen and you cannot close them.
- Third, your passwords no longer work. Cyber criminals will often change your password after hacking your account so they maintain control of it.
- Fourth, your friends or co-workers tell you they are receiving odd messages from your Facebook, Twitter or email accounts that you know you did not send.

- Finally, you believe you may have accidently installed suspicious software. Sometimes you may click on software you did not mean to install, and now you believe you may have infected your computer.

## Wi-Fi



Wi-Fi networks come with their own unique risks, which you need to be aware of. Everything you do over a Wi-Fi network can potentially be monitored. Wireless is like a conversation; without precautions, anyone close to you can listen in on what is said. In addition to eavesdropping, attackers can sometimes use your unsecured connection to compromise your computer or online accounts. As a result, whenever you connect via Wi-Fi you should encrypt all online activity. This is especially important on public Wi-Fi networks, the security of these networks cannot be trusted.

## Working remotely

Technology is enabling more and more of us to work away from the office, either from home or while on the road. This gives you tremendous flexibility but also has certain risks. Ensure that only authorized individuals have access to any system used for your volunteer work. For example children, guests or other household members may not have access to your volunteer files.

While at home or traveling, ensure that any case files or devices with confidential information are physically secure.

- Ensure that any devices you are using are secured. This means making sure the operating system and applications are updated. If your device supports a firewall or anti-virus make sure these are current and are running. Also, make sure your devices are encrypted when possible, this helps secure your data in case your laptop or smartphone is lost or stolen.
- Always be sure to password lock your device whenever you leave it. This protects your device from people walking up to it while you are away and accessing it. Do not allow others to connect devices to your laptop such as their smartphone or USB sticks, as these could be infected as well.

## Mobile device and removable media security

Mobile devices, such as smartphones and tablets, have become incredibly powerful. To protect yourself, we recommend the following:

- Just like with your computer, install only apps that you need and make sure that you download them from trusted sources. In addition do not install apps that request excessive permissions, such as the ability to silently send text messages or copy your address book.
- Just like with your computer, backup your mobile device on a regular basis. This way, if something happens to the device, your information is not lost.

- If you have security software installed, such as anti-virus or a firewall, then make sure they are enabled and updated with the latest version.
- Remember that many of the attacks you find in email can also happen via texting on your mobile device. If a text message seems suspicious or too good to be true, simply delete it.
- Be careful when using Wi-Fi. Many mobile devices will automatically connect to Wi-Fi networks without asking you, putting your device at risk. Disable Wi-Fi if you are not using it.
- Do not access or store ICAB email or other data from our organization on your mobile device or removable media (CD, DVD, memory cards, tapes and flash drives) unless you have been authorized to do so and the appropriate security safeguards are in place.

Finally, when you lose a mobile device anyone can access all of your information including your emails, pictures or contact lists unless it is protected. Protect your devices with a hard-to-guess password or PIN. If your device supports encryption, we recommend you use it.

If you lose a device issued to you by our organization or a device that contained any organizational information, notify your local coordinator immediately.

## Encryption

Encryption is a process that protects your information by making it unreadable or unusable by anyone that does not have your key. A common example of a key is a password, and only people who have that key can decrypt and unlock your

information. To protect your encrypted information you need to protect your key. Examples of things that can be encrypted include the following:

- Mobile devices, such as your laptop, smartphone or USB sticks.
- Communication protocols, such as Voice over IP or Instant Messaging.
- Electronic files or folders.
- Your browser's connections to websites, such as online banking, social networking sites or online shopping.

Passwords

Once someone knows your password, they can steal your identity or access all of your personal information. Let's learn what makes a good password and how to use them securely. There are two key points to good passwords:

- First, you want passwords that are hard to guess. This means do not use simple passwords such as 123456, your pet's name or your birth date.
- Second, use passwords that are easy to remember. If you keep forgetting your passwords they are not very helpful.

To protect yourself, you want your password to be as long as possible. The longer your password is, the stronger it is. In addition to strong passwords, you must protect how you use them:

- Be sure to use different passwords for different accounts. For example, never use the same passwords for your work or bank accounts as the passwords for your personal accounts, such as Facebook, YouTube or Twitter. This way, if one of your passwords is hacked, the other accounts are still safe.


- Never share your password with anyone else, including fellow volunteers. Remember, your password is a secret; if anyone else knows your password it is no longer secure.
- Do not use public computers, such as those at hotels or libraries, to log into ICAB's online data system. Since anyone can use these computers,

they may be infected with malicious code that captures all your keystrokes. Only log in to your account on trusted computers or mobile devices you control.

- If you accidently share your password with someone else or believe your password may have been compromised or stolen, be sure to change it immediately.
- Many online accounts offer something called two-factor authentication, or two-step verification. This is where you need more than just your password to log in, such as codes sent to your smartphone. When possible, always use these stronger methods for authentication.
- If you are no longer using an account, be sure to disable or delete it.
- If you are using ICAB's online data system for case file management and experience issues with your account, notify the ICAB IT staff for assistance.

## Physical security

While much of our training has focused on cyber threats, we cannot forget the physical world. In some ways, it is easier for someone to physically steal our information than it is to steal it digitally. Always make sure that case file documents in your possession are in a locked unit, within another locked unit. For example, keep confidential files in a locked cabinet within a locked room or closet.

To dispose of confidential documents, return them to the local FCRB office for shredding.

## Social Networks

Social networking websites are one of the most exciting technologies on the Internet. What makes these sites so powerful is how easy it is to share with others and to watch and learn what others are doing.

Be careful what information you post. Do not post any confidential information about our organization on any websites. Review the Social Media policy in the ICAB program policies and procedures manual for more information on this topic. If you have any questions about what you can or

cannot post about your involvement with our organization, please ask your local coordinator.

## Protecting your personal computer

To help protect yourself and your family, we recommend you take the following steps to protect any personally owned devices.

Always be sure your computer or mobile devices have the latest patches installed and are running the latest versions of any installed programs, such as your word processor. The simplest way to do this is to enable automatic updates on your computer and mobile devices. In addition, some programs or mobile apps may have their own automatic updating options. If so, be sure they are enabled. If you are no longer using a program, remove or uninstall it.

Make sure your computer's firewall is enabled and you are using updated anti-virus. However, you need to understand that anti-virus only detects and stops known malware. Attackers are constantly developing new malware variants that anti-virus cannot detect. As such, having anti-virus installed does not mean your computer cannot be infected.

Ultimately, you are your own best defense for your computer and mobile devices. Always use common sense. If something seems odd or too good to be true, it may be an attack.

## Personally identifiable information


ICAB handles a great deal of confidential information, including data known as Personally Identifiable Information, commonly called PII. PII is often targeted by attackers because it allows for identity theft or access to other sensitive information.

PII is any information that can identify a specific individual, such as Social Security Numbers, passport numbers, driver's license numbers or any other information that can be used to uniquely identify someone. The same steps provided in the Data Protection section of this handout apply to protecting PII.

## Cloud Computing

Source: http://www.pcmag.com/article2

ICAB has an online data system that stores information about children's cases, as well as the confidential documents for each case. When accessing case information from ICAB's online data system, always be sure you are using your own, unique user ID and password.

In the simplest terms, cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The cloud is just a metaphor for the Internet. For it to be considered "cloud computing," you need to access your data or your programs over the Internet, or at the very least, have that data synchronized with other information over the Web. The end result is the same: with an online connection, cloud computing can be done anywhere, anytime.

As a volunteer with the Iowa Child Advocacy Board:

- Familiarize yourself with the program's confidentiality and social media policies.
- Always understand the sensitivity of the information you are working with. If you are uncertain about the sensitivity of any information or the steps you should take to secure it, ask your local coordinator.
- Only use systems authorized by ICAB to store, process or transmit sensitive information. Do not copy or store sensitive information to any unauthorized systems or accounts, such as personal laptops or personal email accounts.
- Only log into ICAB's online data system with your unique user ID.
- All case file information, digital or hard copy, must be securely stored when in the volunteer's possession.
- If you believe any sensitive data has been lost, stolen or compromised be sure to contact your local coordinator immediately.

## Conclusion

Some key lessons from this handout include:

- Remember you are a target; cyber criminals are attempting to compromise your computers, mobile devices, accounts, and information.
- Be suspicious, if an email or phone call seems odd or too good to be true, it may be an attack.
- Always ensure your computer, mobile devices and applications are updated and running the latest version.
- Always protect our organization's confidential information. Ensure our data is securely stored and only share it with authorized people who have a need to know. When using email or texting, do not use names or other identifying information about a case.

Our goal is not to scare you from using the Internet. Technology is a tremendous tool that enables you to accomplish amazing things. Our goal is simply for you to leverage the latest technology while protecting yourself, your family and our organization.